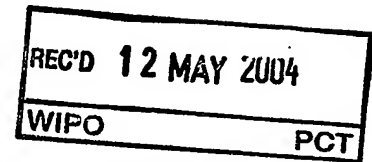


日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 1 9 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 4 0 6 9 2
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 4 0 6 9 2]

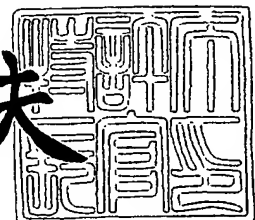
出 願 人 千代田メンテナンス株式会社
Applicant(s):

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 4 年 3 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0030004-02

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60
G06F 19/00

【発明者】

 【住所又は居所】 茨城県鹿島郡旭村箕輪 1 6 3 2 番地 千代田メインテナ
 ンス株式会社内

 【氏名】 井上 義章

【発明者】

 【住所又は居所】 茨城県鹿島郡旭村箕輪 1 6 3 2 番地 千代田メインテナ
 ンス株式会社内

 【氏名】 吉川 祐一

【特許出願人】

 【識別番号】 391051360

 【氏名又は名称】 千代田メインテナンス株式会社

【代理人】

 【識別番号】 100081927

 【弁理士】

 【氏名又は名称】 北條 和由

【手数料の表示】

 【予納台帳番号】 010917

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9723892

【プルーフの要否】 要

【書類名】 明細書
【発明の名称】 偽造品の市場流通を防止する製品認証システム
【特許請求の範囲】

【請求項 1】 インターネットを介して製品の認証を行うシステムで、
認証対象の製品に認証素子として埋め込まれる非接触タグで、製品認証システムの管理者しか知り得ない固有の ID を持ち、ID を電子データとして本体に記録させた非接触タグと、

非接触タグの ID データを読み取るリーダで、製品認証システムの管理者しか知り得ない固有の ID を持ち、ID を電子データとして本体に記録させ、インターネットに接続して通信する手段を持つリーダと、

非接触タグの ID および付帯情報のデータ、非接触タグが埋め込まれた製品情報のデータ、リーダの ID および付帯情報のデータを格納するデータベースで、インターネットに接続して通信する手段を持つデータベースと、

データベースに格納されたデータの読み出しやデータベースへのデータの書き込みを行うデータサーバで、インターネットに接続して通信する手段を持つデータサーバと、

インターネットに接続されたリーダから送信されたリーダの ID データおよび非接触タグの ID データをデータベースに格納されたデータと照合して、リーダおよび非接触タグの認証を行う認証サーバで、インターネットに接続して通信する手段を持つ認証サーバと、で構成される製品認証システムで、

製品認証システムの利用者に非接触タグおよびリーダを配布する前に、データサーバが非接触タグおよびリーダの ID データを読み込み、データファイルを作成してデータベースに格納する手段と、

製品認証システムの利用者に非接触タグおよびリーダが配布された後に、インターネットに接続されたリーダが自分自身の ID データを認証サーバに送信し、認証サーバが受信したリーダの ID データをデータベースに格納されたリーダのデータファイルと照合する手段と、

認証サーバが、同一の ID データとの照合がなされたリーダに対してリーダが認証された旨を通知し、製品に埋め込まれた非接触タグの ID データの送信を促

す手段と、

認証されたリーダが、製品に埋め込まれた非接触タグのIDデータを読み込んで認証サーバに送信し、認証サーバが受信した非接触タグのIDデータをデータベースに格納された非接触タグのデータファイルと照合する手段と、

認証サーバが、同一のIDデータとの照合がなされた非接触タグが認証された旨を、非接触タグのIDデータを送信したリーダに対して通知する手段と、
を備えた製品認証システム。

【請求項2】 アプリケーションサービスプロバイダ（ASP）事業者が管理および運営し、インターネットを介した製品認証サービスをASP方式で提供することを特徴とする、請求項1に記載の製品認証システム。

【請求項3】 リーダの利用者に対して、リーダの管理者および利用者しか知り得ない固有のパスワードを割り当てることにより、利用者側に2重のIDを持させる製品認証システムで、

データサーバが、割り当てられたパスワードのデータを読み込み、配布されたリーダのIDデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する手段と、

認証サーバが、リーダの認証通知後に利用者のパスワード入力を要求し、利用者の端末から入力され送信されたパスワードのデータを受信し、データベースに格納されたデータファイルと照合する手段と、

認証サーバが、同一のパスワードデータとの照合がなされたパスワードが認証された旨を、パスワードデータを送信した利用者端末に対して通知する手段と、
を備えた請求項1または2に記載の製品認証システム。

【請求項4】 製品認証システムの利用者である製品のメーカーに配布されたリーダおよび利用者端末が、製品の名称、型式、製造年月日、製造場所などの製品情報データを非接触タグのIDデータと対応づけてデータサーバに送信する手段と、

データサーバが製品情報データを受信して、埋め込まれた非接触タグのIDデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する手段と、

を備えた請求項1～3の何れかに記載の製品認証システム。

【請求項5】 非接触タグの製造メーカーが、非接触タグのIDと非接触タグの供給先である製品のメーカーを対応づけたデータファイルを作成して、データサーバに送信する手段と、

データサーバが、データファイルを受信してデータベースに格納する手段と、

認証サーバが、リーダから送信された非接触タグのIDデータを受信して、データベースに格納された非接触タグのデータファイルでIDと供給先の対応を照合する手段と、

を備えた請求項1～4の何れかに記載の製品認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、市場に出回る偽造品が流通経路に侵入するのを防ぐことにより、流通経路を形成するメーカー、販売業者、流通業者、消費者の利益を保護するため、流通段階における製品認証サービスをASP方式で提供する製品認証システムに関するものである。

【0002】

【従来の技術】

消費者が腕時計、バッグ、衣類などの装身具を購入するとき、それがどこのメーカーの製品であるかというブランドは商品選びの重要な決め手となる。消費者が装身具に求める価値は、単に必要な機能を満たしているだけでなく、自己表現の手段として優れていることである。ブランドは自己のこだわりを端的に表現するという点で、商品にとって大きな付加価値である。よって、有力なブランドを持つメーカーは、自社製品であることが一目でわかるように、製品に独自の統一されたデザインを施したり、登録商標やロゴマークなどをわざわざ見える位置に表示したりする。消費者はそのような製品を携行するだけで、周囲にメーカーのブランドを誇示して自己のこだわりを表現することができる。このような消費志向にあって、メーカーはシェア拡大を図るために、ブランド力を高めて自社商品の付加価値をより大きくすることに力を注いできた。

【0003】

ところが一方においてこのような消費指向を逆手にとり、付加価値の高いブランド品をそっくり真似て製作された偽造品が市場に出回って、安価に大量に販売されることもままある。偽造品の模倣技術が向上し、取り締まりをのがれて流通経路が巧妙に形成され、ブランド品市場において偽造品が本物の製品である真正品のシェアを奪うようになった。メーカーにとっては自社の製品の売上が落ちるばかりでなく、偽造品が引き起こすトラブルによる信用の低下でブランドの価値を大きく損なうなど、多大な経済的損失を被る。

【0004】

また、偽造品を判別できない販売業者や流通業者は、偽造品を真正品と思い込んで取り扱ってしまう。取扱品が偽造品と発覚したときには不良在庫を大量に抱え込むことになり、偽造品を既に販売していた場合には購入者への保証として偽造品の回収や真正品との交換など、多大な経済的損失を被ることになる。

【0005】

また、偽造品を判別できずに真正品と思い込んで購入した消費者は、購入後にそれが偽造品であるとわかっていても、購入地が海外の旅行先などの場合には返品交渉が困難であり、帰国後に故障などのトラブルが生じてても販売業者の連絡先がわからない、手続きが面倒などの理由で返品や交換ができないため、やはり経済的損失を被ることになる。

以上に述べたように、偽造品はメーカーから販売業者、流通業者を介して消費者に至るまでの、流通経路を形成するものすべてに損害を与える。

【0006】

そこで、メーカーは自社製品と偽造品を判別するために、以下のような対策を講じてきた。

メーカーは、自社製品が真正品であることを特徴づける手段として、製品に高度な技巧を凝らす場合がある。具体的には、素材に型押し加工などを施したり、デザインに形状や色彩の複雑なパターンを設けたり、熟練した手作業による細工を施したり、登録商標やロゴマークなどを特定箇所に配置したりする。これはデザインとしての付加価値を高める効果もあるが、模倣を技術的に困難にして偽造を

防ぐ効果もある。

このような場合の真贋判定は、特徴づけた部分において製品が真正品に十分に似ていれば真正品と判定されるし、十分に似ていなければ偽造品と判定される。

【0007】

また、メーカは、製品を保証するための保証書や保証カードを発行して製品に添付する場合がある。保証書等には固有の製造番号を記載または刻印したり、模倣が技術的に困難な押印や透かしなどの技巧を施したりする。

このような場合の真贋判定は、製品に保証書等が添付されており、その保証書等が真正の保証書等に十分に似ていれば真正品と判定されるし、十分に似ていなければ偽造品と判定される。

【0008】

さらに、メーカは、模倣が技術的に困難なホログラムなどを施したシールを用いて製品の包装を封印し、容易に開封されない工夫を施す場合がある。

このような場合の真贋判定は、製品の包装を封印したシールを開封した形跡がなければ真正品と判定されるし、開封した形跡があれば偽造品と判定される。

【0009】

【発明が解決しようとする課題】

これまでに述べた従来の方法によって、ある製品が真正品であるか偽造品であるかを判別して真正品を認証する場合に、以下のような問題がある。

まず、デザインの技巧や登録商標などの表示は、模倣精度を高めれば十分に真正品に似せることができる。よって、判別のためには微妙な違いを見極めるための専門的な知識や技能が必要となり、判別者を養成したり雇い入れたりしなければならない。それでも真正品と模造品の見分けがつかなければ判別はできない。

【0010】

また、製品に添付する保証書の場合も同様に、模倣精度を高めれば十分に真正の保証書に似せることができる。よって、偽造品に添付された偽造保証書が真正品に添付された真正保証書と見分けがつかなければ、真正品と偽造品の判別ができない。さらに、押印や透かしなどの技巧を施した場合は、違いを見極めるための専門的な知識や技能が新たに必要となり、専門知識や技能が十分でない、一

見似ている程度の模倣でも安易に信用してしまうなどの逆効果もある。

【0011】

さらに、包装をホログラムなどの技巧を施したシールで封印した場合は、購入者が購入前に開封できないために内容物を吟味できず、購買意欲の低下を招くというデメリットが生じる。また、シールの製造に余分なコストが掛かる。さらに、上記保証書の場合と同様にホログラムなどの技巧を施した場合は、判別のための専門的な知識や技能が新たに必要となり、専門知識や技能が十分でないと、一見似ている程度の偽造シールでも判別できない。

【0012】

以上の理由から、製品自体、保証書、封印シールなどの外観上の違いを人為的に判別するという従来の方法は、判別のための専門的な知識や技能を必要とする上に判別作業時間を要する。よって、流通段階において、低コストで容易に任意の場所において短時間で大量に正確に判別することはできない。

【0013】

本発明は、前記従来における商品流通市場での真性品と偽造品との判別の課題に鑑み、商品の真贋の判別基準を外観上の差異以外に設け、さらに判別方法は人為的な作業ではなく機械的な処理によって効率よく行うようにすることが出来、また商品を取り扱う流通業者や販売点がインターネットを介して簡便に真贋判定を利用出来るようにすることを目的とするものである。

【0014】

【課題を解決するための手段】

本発明では前記のような目的を達成するため、以下のような製品認証システムを確立するものである。

製品認証システムを構成するハードウェアとして、非接触タグ、リーダー、データベース、データサーバ、認証サーバを用意する。

【0015】

非接触タグは、認証対象の製品に認証素子として埋め込まれるもので、製品認証システムの管理者しか知り得ない固有のIDを持ち、IDを電子データとして本体に記録させる。

リーダは、非接触タグのIDデータを読み取るもので、製品認証システムの管理者しか知り得ない固有のIDを持ち、IDを電子データとして本体に記録させ、インターネットに接続して通信する手段を持つ。

【0016】

データベースは、非接触タグのIDおよび付帯情報のデータ、非接触タグが埋め込まれた製品情報のデータ、リーダのIDおよび付帯情報のデータを格納するもので、インターネットに接続して通信する手段を持つ。

データサーバは、データベースに格納されたデータの読み出しやデータベースへのデータの書き込みを行うもので、インターネットに接続して通信する手段を持つ。

【0017】

認証サーバは、インターネットに接続されたリーダから送信されたリーダのIDデータおよび非接触タグのIDデータをデータベースに格納されたデータと照合して、リーダおよび非接触タグの認証を行うもので、インターネットに接続して通信する手段を持つ。

【0018】

このようなハードウェアを使用し、以下のような手順で製品の真性品であるか否かの認証を行う。

まず、製品認証システムの利用者に非接触タグおよびリーダを配布する前に、データサーバが非接触タグおよびリーダのIDデータを読み込み、データファイルを作成してデータベースに格納する。

【0019】

製品認証システムの利用者に非接触タグおよびリーダが配布された後に、インターネットに接続されたリーダが自分自身のIDデータを読み込んで認証サーバに送信し、認証サーバが受信したリーダのIDデータをデータベースに格納されたリーダのデータファイルと照合する。

【0020】

認証サーバが、同一のIDデータとの照合がなされたリーダに対してリーダが認証された旨を通知し、製品に埋め込まれた非接触タグのIDデータの送信を促

す。

認証されたリーダが、製品に埋め込まれた非接触タグの I D データを読み込んで認証サーバに送信し、認証サーバが受信した非接触タグの I D データをデータベースに格納された非接触タグのデータファイルと照合する。

【0021】

認証サーバが、同一の I D データとの照合がなされた非接触タグが認証された旨を、非接触タグの I D データを送信したリーダに対して通知する。

また、上記の製品認証システムをアプリケーションサービスプロバイダ (A S P) 事業者が管理および運営して、インターネットを介した製品認証サービスを A S P 方式で提供することもできる。

【0022】

また、上記の製品認証システムにおいて、リーダの利用者に対してリーダの管理者および利用者しか知り得ない固有のパスワードを割り当てることにより、利用者側に 2 重の I D を持たせた場合には、以下の手順を加えることにより製品認証システム全体で 3 重のチェック機能を持たせることができる。

【0023】

データサーバが、割り当てられたパスワードのデータを配布されたリーダの I D データと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する。

認証サーバが、リーダの認証通知後に利用者のパスワード入力を要求し、利用者の端末から入力され送信されたパスワードのデータを受信し、データベースに格納されたデータファイルと照合する。

認証サーバが、同一のパスワードデータとの照合がなされた場合に、パスワードが認証された旨をパスワードデータを送信した利用者端末に対して通知する。

【0024】

また、上記の製品認証システムに以下の手順を加えることができる。

製品認証システムの利用者である製品のメーカに配布されたリーダおよび利用者端末が、製品の名称、型式、製造年月日、製造場所などの製品情報データを非接触タグの I D データと対応づけてデータサーバに送信する。

データサーバが製品情報を受信して、埋め込まれた非接触タグのIDデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する。

【0025】

上記の手順を加えることにより、例えば安価な真正品に取り付けられた非接触タグの埋め込み部分を取り外して、真正品とは別の高価な製品を模倣した偽造品に取り付け、偽造品の認証を受けて販売しようとする場合に、非接触タグのID以外に製品名称や型式などの製品情報を参照することにより、上記のような悪用を防ぐことができる。なお、ここで言う「メーカ」とは、製造元以外に、発売元や輸入元等を指す。

【0026】

さらに、上記の製品認証システムに以下の手順を加えることができる。

非接触タグの製造メーカが、非接触タグのIDと非接触タグの供給先である製品のメーカを対応づけたデータファイルを作成して、データサーバに送信する。

データサーバが、データファイルを受信してデータベースに格納する。

認証サーバが、リーダから送信された非接触タグのIDデータを受信して、データベースに格納された非接触タグのデータファイルでIDと供給先の対応を照合する。

【0027】

以上の手順によって、製品の認証が2段階になる。つまり、はじめに非接触タグのIDと供給先との対応を確認し、後に非接触タグのIDと製品情報との対応を確認することになるため、偽造品の検出をより効率的に行うことができると同時に、より信頼度を高めることができる。

【0028】

【発明の実施の形態】

次に、図面を参照しながら、本発明の実施の形態について、具体的且つ詳細に説明する。

まず、本発明による製品認証システムの一実施態様について、その概要を図1を参照しながら説明する。

【0029】

製品認証システムの当事者は、管理者であるASP事業者10、利用者であるメーカ20、販売業者30、流通業者40、消費者50である。ASP事業者10は、非接触タグ11およびリーダ12を管理して製品認証システムを管理・運営し、製品認証サービスを提供する。

【0030】

ASP事業者10は、メーカ20に対して非接触タグ11を供給する。非接触タグ11は固有のIDを持ち、IDが電子データとして本体に記録されているものである。ASP事業者10は、非接触タグ11のIDデータおよび供給先であるメーカ名などの付帯情報のデータを管理する。

【0031】

上記の非接触タグ11の供給については、非接触タグ11の製造メーカが、メーカ20に直接非接触タグ11を供給することもできる。この場合は、非接触タグ11の製造メーカが、非接触タグ11のIDと供給先である商品のメーカ20を対応づけたデータファイルを作成して、ASP事業者10にデータを提供することもできる。

【0032】

非接触タグ11としては、通信機能付き超小型ICチップを使用することが出来る。このような通信機能付き超小型ICチップとしては、例えば日立製作所製の商品名ミューチップ(μチップ)を挙げることが出来る。このチップは、縦と横がそれぞれ0.4mm、厚さは約170μmと指先に載せてもほんの点にしか見えない。その中に一二ビットのメモリーと二・四五ギガヘルツの電波で通信できる機能を有する。

【0033】

ASP事業者10は、製品認証サービスの各利用者に対して前記非接触タグ11のICコードを読み取るリーダ12を貸与する。リーダ12は、パソコンなどの汎用の端末装置を介してインターネットに接続することができ、固有のIDを持ち、IDが電子データとして本体に記録されているものである。ASP事業者10は、リーダ12のIDデータおよび貸与先である利用者名などの付帯情報のデータを管理する。

【0034】

ASP事業者10は、リーダ12の貸与に際し、利用者に対して固有のパスワードを割り当てることにより、利用者側に2重のIDを持たせることもできる。ASP事業者10は、割り当てたパスワードのデータをリーダ12の付帯情報のデータとして管理する。

【0035】

メーカ20は、ASP事業者10から供給された非接触タグ11を製品に埋め込む。外観上はわからないように製品の内部に埋め込むことで、製品の美観を損ねることがなく、取り外して悪用されるのを防止できる。メーカ20は、貸与されたリーダ12をインターネットに接続する。メーカ20は、リーダ12の認証を受けた上で、非接触タグ11に対応する製品の名称、製造年月日、製造場所などの製品情報をASP事業者10に登録する。ASP事業者10は、非接触タグ11のID、供給先であるメーカ名に加えて、メーカ20から登録された製品情報のデータを対応づけて管理する。

メーカ20は、リーダ12の認証を受けた上で、登録したデータを閲覧することができる。

【0036】

販売業者30および流通業者40は、貸与されたリーダ12をインターネットに接続する。販売業者30および流通業者40は、リーダ12の認証を受けた上で、取り扱う製品が真正品であることの認証をASP事業者10に照会する。ASP事業者10は、照会された非接触タグ11のIDデータと管理するデータとを照合して製品の認証を行い、販売業者30および流通業者40に通知する。

【0037】

消費者50は製品の購入時に、販売業者30に対して、販売業者30がその製品に対して認証を取得したという証拠の提示を要求することができる。販売業者30は消費者50に対して、その製品の認証を取得したという証拠を提示する。消費者50は、新品の購入時に限らず中古品の売買時においても、任意の販売業者30に対して製品認証を要求し、製品認証を取得した証拠の提示を要求することができる。

【0038】

次に、本発明による製品認証システムの前記実施態様を実現するハードウェアの構成について、図2を参照しながら説明する。

製品認証サービスの提供者であるASP事業者10は、インターネット上でデータの受け渡しをするためのデータベース13、データサーバ14、認証サーバ15を管理する。

【0039】

製品認証サービスの利用者であるメーカ20、販売業者30、流通業者40は、ASP事業者10から貸与されたリーダ12を保持し、リーダ12をインターネットに接続するためのパソコンなどの汎用端末装置21、31、41を持つ。

ASP事業者10は、メーカ20に非接触タグ11を供給する。メーカ20は、非接触タグ11を埋め込んだ製品を、販売業者30あるいは流通業者40に出荷する。

販売業者30および流通業者40は、流通段階で製品を取扱い、販売業者30は最終的に消費者50に製品を販売する。

【0040】

次に、本発明による製品認証システムの前記実施態様を実現するため、前記ハードウェアにより行われる情報の処理について、図3を参照しながら詳細に説明する。

まず、メーカ20による製品情報の登録、閲覧は以下の手順で行われる。

メーカ20は、非接触タグ11を埋め込んで製造した製品の名称、製造年月日、製造場所などの製品情報をもとにデータファイルを作成する。メーカ20は、端末装置21を介してリーダ12をインターネットに接続する。リーダ12は、自分自身のIDデータを認証サーバ15に送信する。認証サーバ15は、受信したリーダ12のIDデータを、データベース13に格納されたリーダ12のデータファイルと照合する。照合されれば認証サーバ15は自動的にメーカ20の端末装置21にリーダ12の認証を通知する。

【0041】

さらに、パスワードが割り当てられている場合は、認証サーバ15がパスワー

ドを要求し、入力されたパスワードデータをデータベース 13 のデータファイルと照合して、照合されれば利用者の認証を通知する。

それからメーカ 20 は、データサーバ 14 に対して製品情報の登録を要求し、非接触タグ 11 の ID と対応させながら製品情報データファイルを送信する。データサーバ 14 は、受信した製品情報データファイルを予め登録してあった非接触タグ 11 のデータファイルと対応づけて非接触タグ 11 のデータファイルを更新し、データベース 13 に格納する。

【0042】

メーカ 20 は、リーダ 12 の認証、パスワードの認証を受けた上でデータサーバ 14 に対して製品情報の閲覧を要求する。データサーバ 14 はデータベース 13 から非接触タグ 11 のデータファイルを読み出して、製品情報データをメーカ端末 21 に送信する。メーカ 20 はメーカ端末 21 上で製品情報を閲覧する。

【0043】

次に、販売業者 30 および流通業者 40 による製品の認証取得は以下の手順で行われる。

まず販売業者 30 および流通業者 40 は端末装置 31、41 を介してリーダ 12 をインターネットに接続する。リーダ 12 は、自分自身の ID データを認証サーバ 15 に送信する。認証サーバ 15 は、受信したリーダ 12 の ID データを、データベース 13 に格納されたリーダ 12 のデータファイルと照合する。照合されれば認証サーバ 15 は自動的に販売業者 30 および流通業者 40 の端末装置 31、41 にリーダ 12 の認証を通知する。

【0044】

さらに、パスワードが割り当てられている場合は、認証サーバ 15 がパスワードを要求し、入力されたパスワードデータをデータベース 13 のデータファイルと照合して、照合されれば利用者の認証を通知する。

それから販売業者 30 および流通業者 40 は、受け取った製品が真正品であることを確認するために、リーダ 12 で製品に埋め込まれた非接触タグ 11 の ID を読み取る。すると認証サーバ 15 は自動的に非接触タグ 11 の ID を読み取り、データベース 13 に格納された非接触タグ 11 のデータファイルと照合する。

このとき、認証サーバ15は非接触タグ11のIDと供給先であるメーカ20との対応を確認することによって、偽造品の判別を行うこともできる。照合されれば認証サーバ15は、自動的に販売業者30および流通業者40の端末装置31、41に非接触タグ11の認証を通知するとともに、付帯情報として管理されている製品の型式など製品情報の一部を開示する。販売業者30および流通業者40は、開示された製品の型式などの製品情報と認証された製品を比較して、製品が真正品であることを確認する。

【0045】

仮に、製品認証システムを不正に利用しようとした場合について、図4を参照しながら説明する。

まず、正規に利用する場合について説明すると、ASP事業者10と契約して製品認証サービスを受ける正規の販売業者30は、ASP事業者10から貸与されたリーダ12が持つ固有のIDにより、自動的にリーダ12の認証を受けることができる。さらに、この販売業者30にASP事業者10からパスワードが割り当てられている場合は、パスワードの照合によって利用者の認証を受けることができる。販売業者30は真正品に埋め込まれた非接触タグ11のIDをリーダ11で読み取ることによって、自動的に製品の認証を受けることができる。製品が偽造品であれば、非接触タグ11が埋め込まれていないために製品の認証は受けられず、自動的に偽造品を判別することができる。

【0046】

次に、不正利用者がASP事業者10から正規の利用者に貸与されたリーダ12を盗んで製品認証システムを不正に利用しようとした場合について説明する。不正業者は自動的にリーダ12の認証を受けることができるが、ASP事業者10からパスワードを要求された場合には、正規利用者に割り当てられたパスワードを知らないので正しいパスワードを入力できないため、利用者の認証を受けることができない。よって、不正利用者は製品認証サービスを受けられない。

【0047】

さらに、不正利用者がリーダを偽造して製品認証システムを不正に利用しようとした場合について説明すると、不正利用者は偽造リーダをインターネットに接

続しても、ASP事業者10からリーダの認証を受けることができない。よって、不正利用者は製品認証サービスを受けられない。

【0048】

【発明の効果】

以上説明した通り、本発明では、製品の真贋判別基準を従来の外観以外に設けること、真贋判別作業を従来の人為的な目視判断に依らず機械的な電子情報処理作業に依ることを課題とし、それらを解決した製品認証システムをインターネット上に構築し、製品の流通経路を形成するメーカ、販売業者、流通業者に対して、インターネット上の製品認証サービスとしてASP方式で提供することにより、メーカの工場出荷から小売店の店頭入荷に至るまでの製品の流通段階ごとに、低コストで容易に任意の場所において短時間で大量に正確に、真正品と偽造品の判別が実現できる。

【0049】

また、上記の製品認証システムにおいて、リーダに固有のIDを持たせ、さらに利用者に固有のパスワードを割り当てて管理することにより、リーダの盗難や偽造による製品認証システムの不正利用を防止することができる。

したがって、市場に出回る偽造品が流通経路に侵入するのを防ぎ、製品を製造するメーカをはじめとして、製品を取り扱う販売業者および流通業者、製品を購入する消費者に至るまで、製品に関わり流通経路を形成するすべての製品認証システム利用者の利益を保護することができる。

【図面の簡単な説明】

【図1】

本発明による製品認証システムの一実施形態の概要を説明した図で、ものおよび情報の流れを示すことによりシステムの当事者の役割を説明する。

【図2】

前記製品認証システムの実施形態を実現するために必要なハードウェアの構成を説明した図で、当事者ごとに具備すべきハードウェアを示す。

【図3】

前記図2に示したハードウェアにより製品認証システムの実施形態を実現する

ための情報処理について詳細に説明した図で、ハードウェア間でやりとりされる情報の内容および方向を示す。

【図 4】

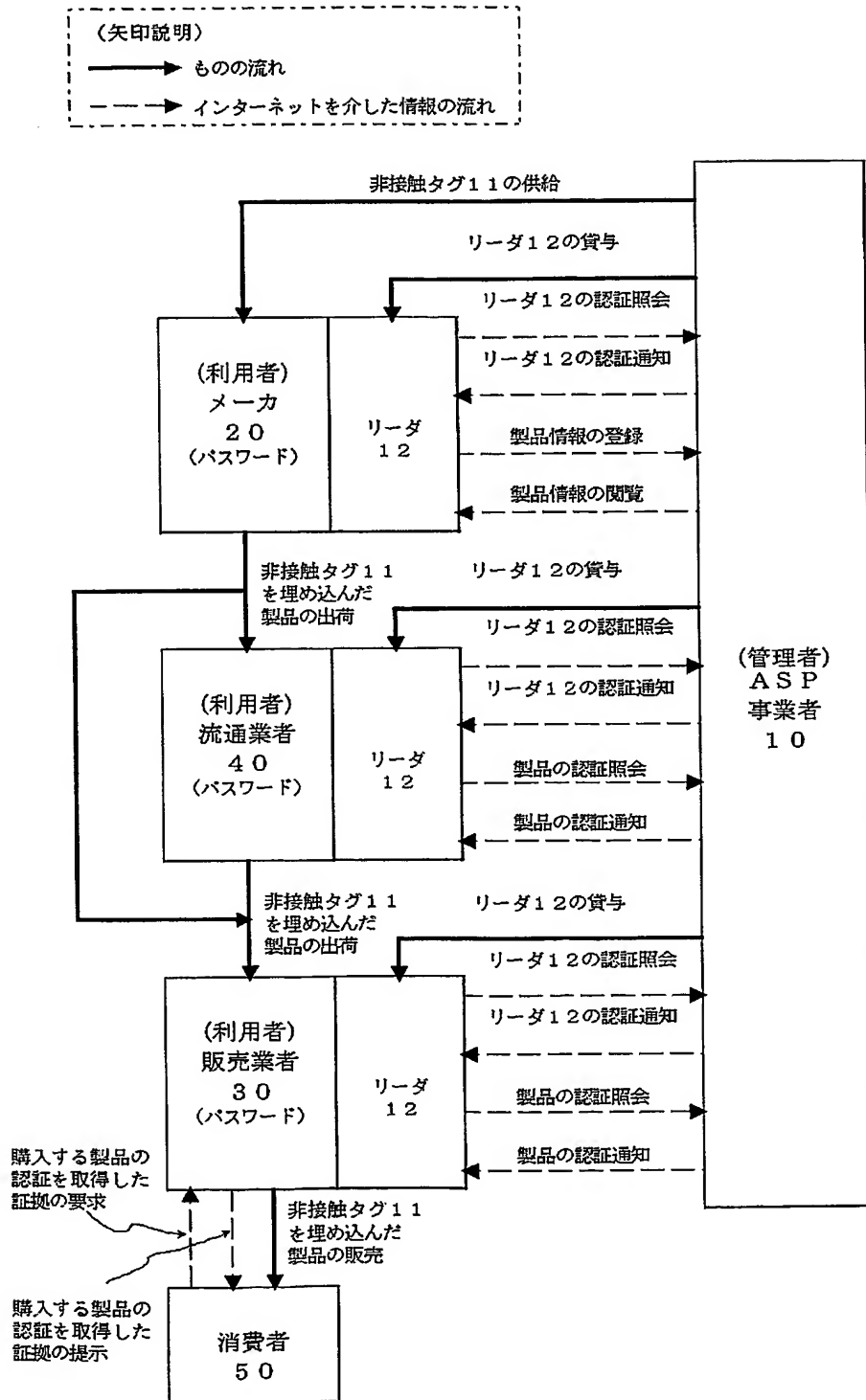
前記製品認証システムを不正に利用しようとした場合の製品認証システムの応答について、正常に利用した場合と比較して説明した図である。

【符号の説明】

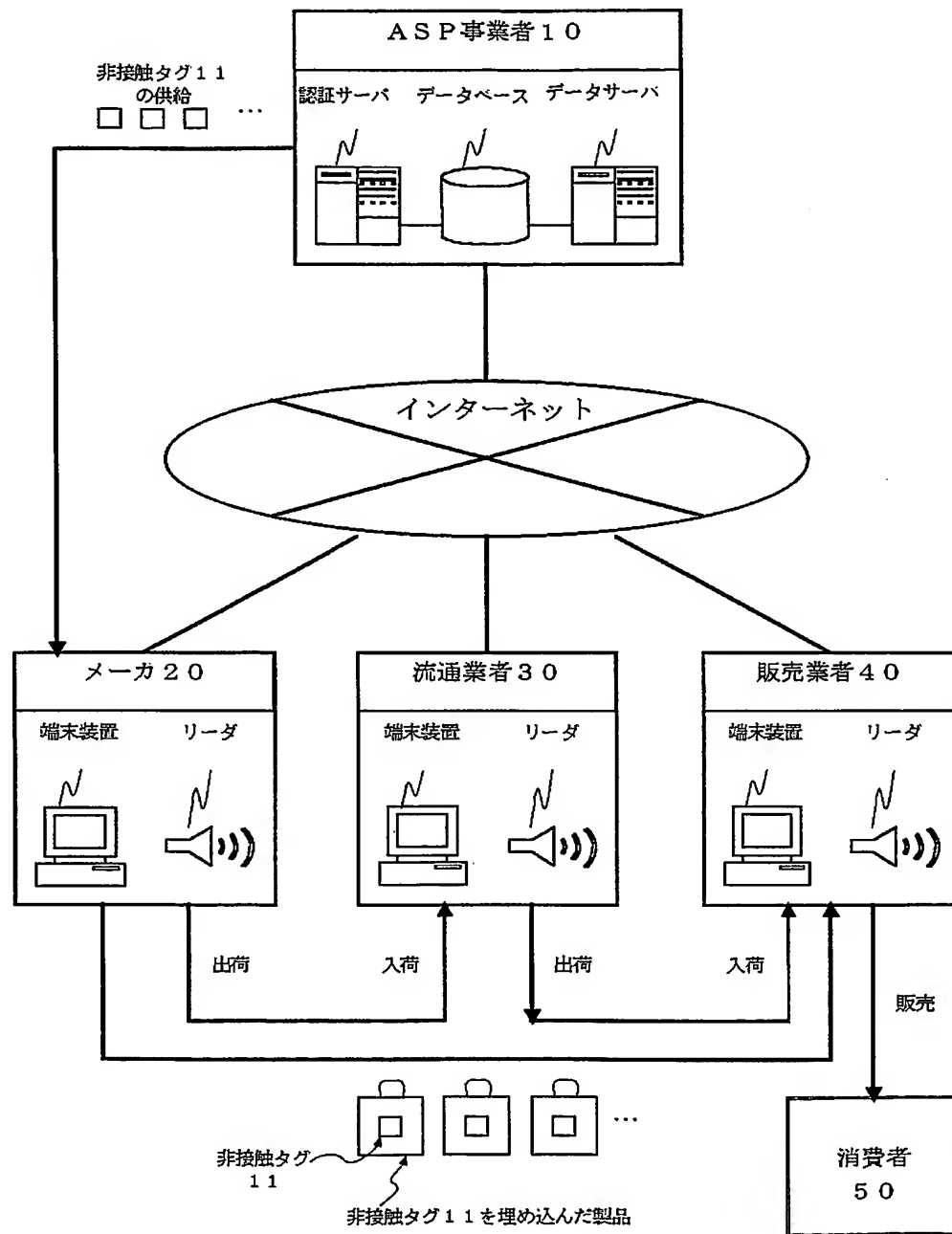
- 10 ASP
- 11 非接触タグ
- 12 リーダ
- 13 データベース
- 14 データサーバ
- 15 認証サーバ
- 20 メーカ
- 21 メーカのインターネット接続のための汎用端末装置
- 30 販売業者
- 31 販売業者のインターネット接続のための汎用端末装置
- 40 流通業者
- 41 流通業者のインターネット接続のための汎用端末装置
- 50 消費者

【書類名】 図 面

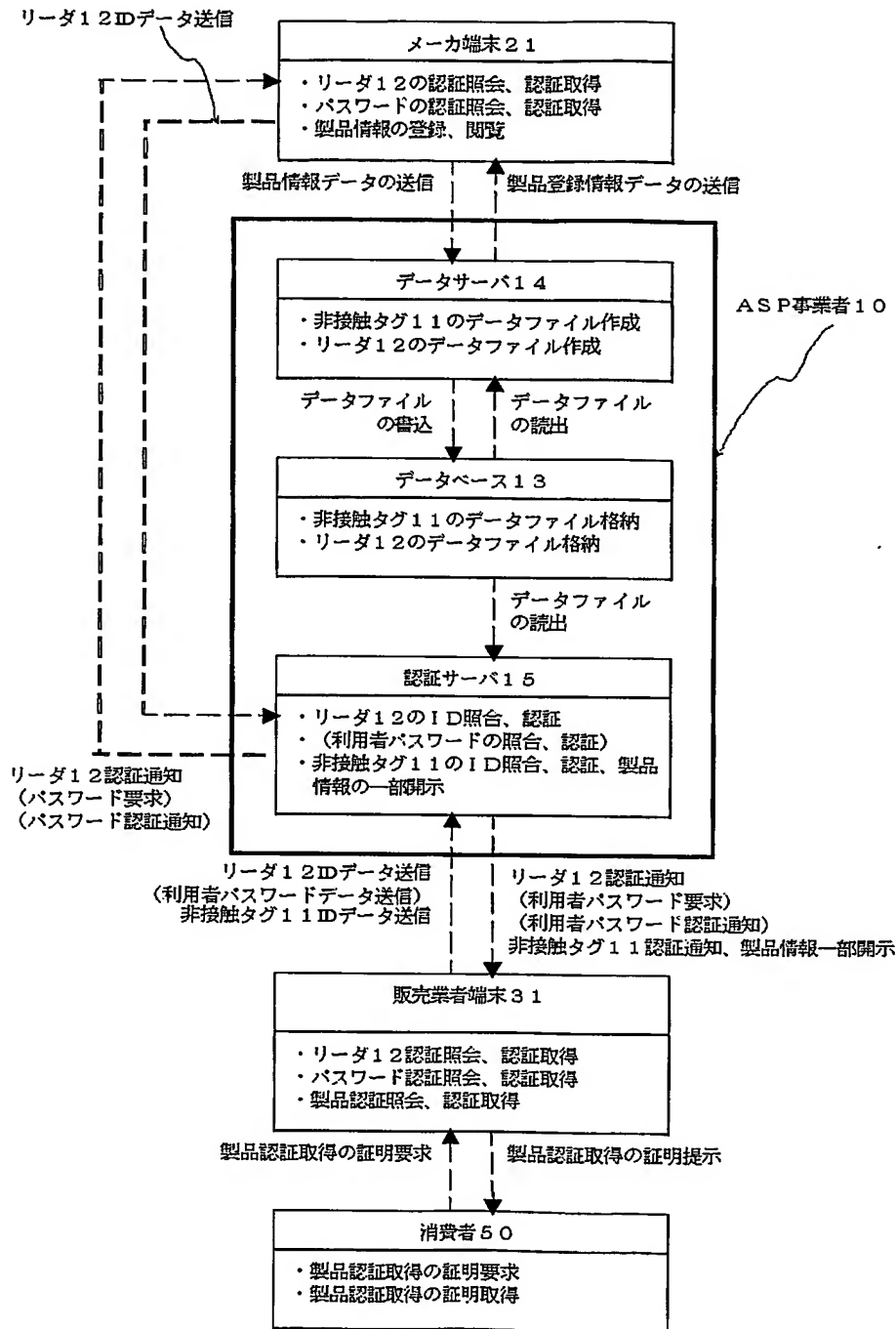
【図 1】



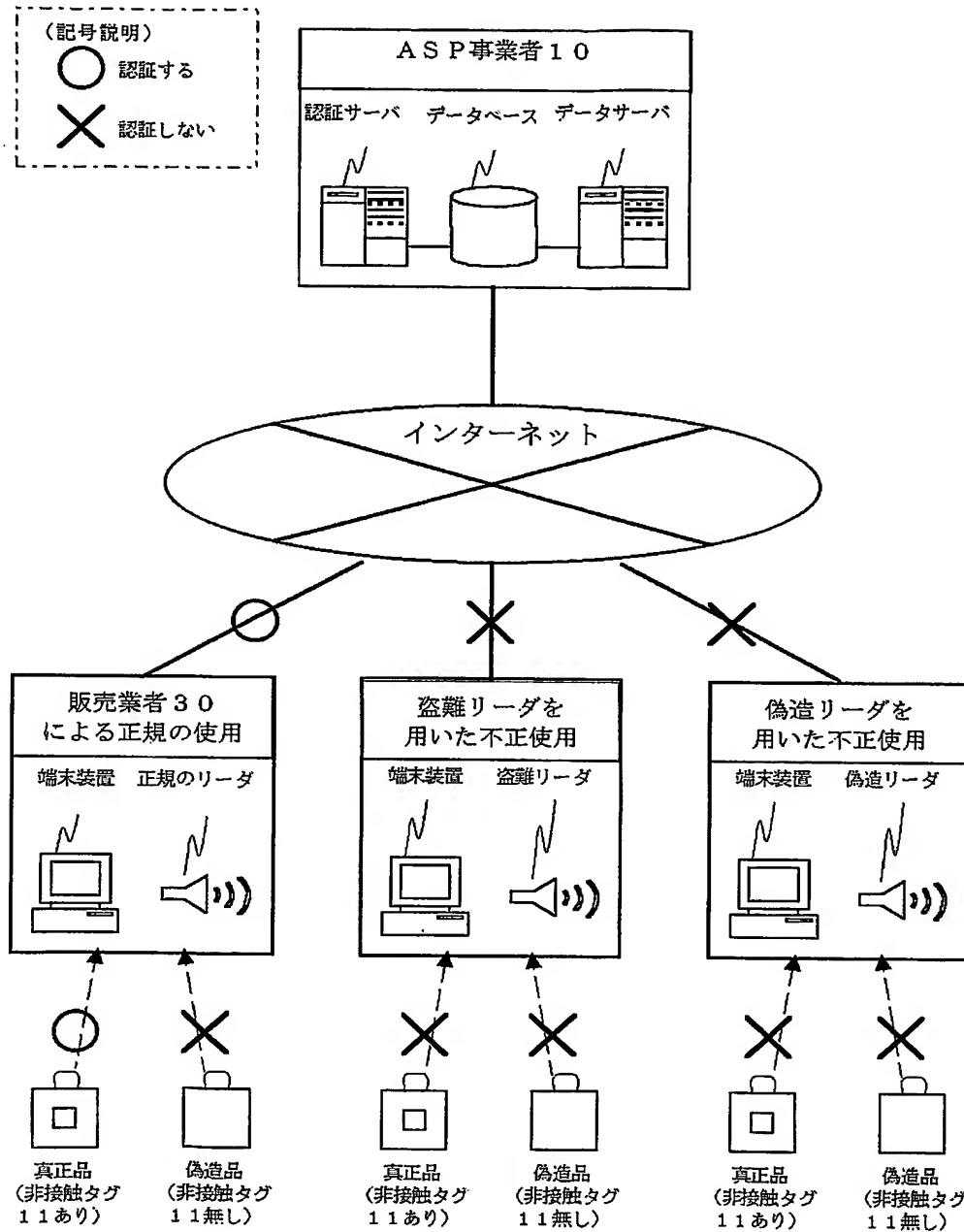
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 市場に出回る偽造品が流通経路に侵入するのを防ぐ。

【解決手段】 データサーバが非接触タグ 11 およびリーダ 12 の ID データを読み込み、データファイルを作成してデータベースに格納する。インターネットに接続されたリーダ 12 が自分自身の ID データを読み込んで認証サーバに送信し、認証サーバが受信したリーダ 12 の ID データをデータベースに格納されたリーダ 12 のデータファイルと照合し、一致すればリーダ 12 を認証する。認証されたリーダ 12 が、製品に埋め込まれた非接触タグ 11 の ID データを読み込んで認証サーバに送信し、認証サーバが受信した非接触タグ 11 の ID データをデータベースに格納された非接触タグのデータファイルと照合し、その結果一致すれば認証された旨をリーダ 12 に通知する。この製品認証システムは、アプリケーションサービスプロバイダ (ASP) 事業者 10 が管理および運営する。

【選択図】 図 2

職権訂正履歴 (職権訂正)

特許出願の番号	特願 2003-040692
受付番号	50300261285
書類名	特許願
担当官	末武 実 1912
作成日	平成15年 2月21日

<訂正内容1>

訂正ドキュメント

書誌

訂正原因

職権による訂正

訂正メモ

【特許出願人】の欄の記載に誤りがあり訂正します。

訂正前内容

【特許出願人】

【住所又は居所】 391051360

【氏名又は名称】 千代田メンテナンス株式会社

訂正後内容

【特許出願人】

【識別番号】 391051360

【氏名又は名称】 千代田メンテナンス株式会社

次頁無

認定・付加情報

特許出願の番号	特願 2003-040692
受付番号	50300261285
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 3月 4日

<認定情報・付加情報>

【提出日】	平成15年 2月19日
【特許出願人】	
【識別番号】	391051360
【住所又は居所】	茨城県鹿島郡旭村箕輪 1 6 3 2 番地
【氏名又は名称】	千代田メンテナンス株式会社
【代理人】	申請人
【識別番号】	100081927
【住所又は居所】	茨城県水戸市千波町 2 4 3 2 番地の 3 7
【氏名又は名称】	北條 和由

次頁無

特願 2 0 0 3 - 0 4 0 6 9 2

出 願 人 履 歴 情 報

識別番号

[3 9 1 0 5 1 3 6 0]

1. 変更年月日

1 9 9 7 年 2 月 2 8 日

[変更理由]

住所変更

住 所

茨城県鹿島郡旭村箕輪 1 6 3 2 番地

氏 名

千代田メンテナンス株式会社